

DENISE M. MINGRONE
(STATE BAR NO. 135224)
dmingrone@orrick.com
ROBERT L. URIARTE
(STATE BAR NO. 258274)
ruriarte@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025-1015
Telephone: +1 650 614 7400
Facsimile: +1 650 614 7401

Attorneys for Plaintiff/Counterdefendant
SYNOPSISYS, INC.

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

SYNOPSISYS, INC.,

Plaintiff,

v.

UBIQUITI NETWORKS, INC., UBIQUITI
NETWORKS INTERNATIONAL LIMITED,
CHING-HAN TSAI, and DOES 1-20,
inclusive,

Defendants.

Case No. 3:17-cv-00561-WHO

**SYNOPSISYS, INC.'S OPPOSITION TO
DEFENDANTS' RULE 12(b)(6)
MOTION TO DISMISS**

Date: May 17, 2017
Time: 2:00 p.m.
Dept. Courtroom 2, 17th Floor
Judge: Hon. William H. Orrick

UBIQUITI NETWORKS, INC.

Counterclaimant,

v.

SYNOPSISYS, INC.,

Counterdefendant.

TABLE OF CONTENTS

	Page
INTRODUCTION	1
LEGAL STANDARD	2
FACTUAL BACKGROUND	2
ARGUMENT	4
I. SYNOPSISYS PROPERLY ALLEGES ALL OF ITS DMCA CLAIMS	4
A. The FAC States Many Violations of DMCA Sections 1201(a)(2) and 1201(b)	4
B. Synopsisys' License Key System Protects its Reproduction Right	6
II. SYNOPSISYS PROPERLY ALLEGES THAT DEFENDANTS TRAFFICKED COUNTERFEIT AND ILLICIT LABELS	7
III. SYNOPSISYS ALLEGES RICO CLAIMS AGAINST ALL DEFENDANTS	10
A. The FAC Alleges Counterfeit Access Device Use and Trafficking	11
B. The FAC Alleges Criminal Copyright Infringement	14
C. The FAC Alleges Use of Interstate Wires in Furtherance of the Enterprise	16
D. The FAC Alleges a Pattern of Racketeering Activity	18
E. The FAC Alleges Distinct RICO Enterprises	19
IV. SYNOPSISYS ALLEGES A RICO CONSPIRACY	21
V. SYNOPSISYS ADEQUATELY ALLEGES FRAUD AND NEGLIGENT MISREPRESENTATION	21
CONCLUSION	25

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Airframe Systems, Inc. v. Raytheon Co.</i> , 520 F. Supp. 2d 258 (D. Mass. 2007)	6
<i>Allwaste, Inc. v. Hecht</i> , 65 F.3d 1523 (9th Cir. 1995).....	18, 19
<i>Andrews Farms v. Calcot, Ltd.</i> , 527 F. Supp. 2d 1239 (E.D. Cal. 2007).....	24
<i>Apollo Capital Fund, LLC v. Roth Capital Partners, LLC</i> , 158 Cal. App. 4th 226 (2007).....	21
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009)	2
<i>Ass’n for Info. Media & Equip. v. Regents of the Univ. of Cal.</i> , No. 2:10-cv-09378-CBM-MAN, Dkt. No. 21-5 (C.D. Cal. Feb. 15, 2011)	5
<i>Ass’n for Info. Media & Equip. v. Regents of the Univ. of Cal.</i> , 2012 WL 7683452 (C.D. Cal. Nov. 20, 2012).....	5
<i>Barnes & Noble, Inc. v. LSI Corp.</i> , 849 F. Supp 2d 925 (N.D. Cal. 2012)	24
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007)	2
<i>Bennett v. Berg</i> , 685 F.2d 1053 (8th Cir. 1982).....	20
<i>Blake v. Dierdorff</i> , 856 F.2d 1365 (9th Cir. 1988).....	22
<i>Bryant v. Mattel, Inc.</i> , 573 F. Supp. 2d 1254 (C.D. Cal. 2007).....	15
<i>Chaghouri v. Wells Fargo Bank, N.A.</i> , 2015 WL 65291 (N.D. Cal. Jan. 5, 2015)	25
<i>Cheek v. United States</i> , 498 U.S. 192 (1991)	14
<i>Cisco Systems, Inc. v. STMicroelectronics, Inc.</i> , 77 F. Supp. 3d 887 (N.D. Cal. 2014)	23

1	<i>Compliance Servs. of Am., LLC v. Houser Holdings, LLC,</i>	
2	2013 WL 4169119 (N.D. Cal. Aug. 9, 2013).....	24
3	<i>Ctr. for Biological Diversity v. Salazar,</i>	
4	695 F.3d 893 (9th Cir. 2012).....	6
5	<i>Duncan v. Walker,</i>	
6	533 U.S. 167 (2001).....	6
7	<i>Ferleger v. First Am. Mortg. Co.,</i>	
8	662 F. Supp. 584 (N.D. Ill. 1987)	22
9	<i>Flood v. Makowski,</i>	
10	2004 WL 1908221 (M.D. Pa. Aug. 24, 2004)	23
11	<i>Glendale Fed. Sav. & Loan Ass’n v. Marina View Heights Dev. Co.,</i>	
12	66 Cal. App. 3d 101 (1977).....	24
13	<i>GreenCycle Paint, Inc. v. PaintCare, Inc.,</i>	
14	2017 U.S. Dist. LEXIS 55314 (N.D. Cal. Apr. 11, 2017)	2
15	<i>H.J. Inc. v. Northwestern Bell Tel. Co.,</i>	
16	492 U.S. 229 (1989).....	15, 18, 19
17	<i>Haroco, Inc. v Am. Nat. Bank and Trust Co. of Chicago,</i>	
18	747 F.2d 384 (7th Cir. 1984).....	23
19	<i>Ice Cream Distribs. of Evansville, LLC v. Dreyer’s Grand Ice Cream, Inc.,</i>	
20	2010 U.S. Dist. LEXIS 99930 (N.D. Cal. Sept. 10, 2010).....	20
21	<i>ICONICS, Inc. v. Massaro,</i>	
22	192 F. Supp. 3d 254 (D. Mass. 2016)	15
23	<i>Kearney v. Foley & Lardner, LLP,</i>	
24	607 F. App’x 757 (9th Cir. 2015)	18, 19
25	<i>Lazar v. Superior Court,</i>	
26	12 Cal. 4th 631 (1996)	21
27	<i>Locke v. Warner Bros., Inc.,</i>	
28	57 Cal. App. 4th 354 (1997).....	21
	<i>MAI Sys. Corp. v. Peak Computer, Inc.,</i>	
	991 F.2d 511 (9th Cir. 1993).....	6
	<i>Menjivar v. Trophy Props. IV DE, LLC,</i>	
	2006 WL 2884396 (N.D. Cal. Oct. 10, 2006).....	25
	<i>Microsoft Corp. v. # 9 Software, Inc.,</i>	
	2005 U.S. Dist. LEXIS 36710 (E.D. Va. Dec. 15, 2005).....	7, 9

1	<i>Microsoft Corp. v. A Plus Open LLC,</i>	
2	2007 U.S. Dist. LEXIS 8435 (D. Colo. Feb. 6, 2007)	7, 9
3	<i>Microsoft Corp. v. AGA Solutions, Inc.,</i>	
4	2010 U.S. Dist. LEXIS 26756 (E.D.N.Y. Mar. 22, 2010)	7
5	<i>Microsoft Corp. v. Buy More, Inc.,</i>	
6	136 F. Supp. 3d 1148 (C.D. Cal. 2015).....	7
7	<i>Microsoft Corp. v. EEE Bus., Inc.,</i>	
8	555 F. Supp. 2d 1051 (N.D. Cal. 2008)	7
9	<i>Microsoft Corp. v. Ion Techs. Corp.,</i>	
10	484 F. Supp. 2d 955 (D. Minn. 2007)	7, 8, 10
11	<i>Microsoft Corp. v. Pronet Cyber Techs., Inc.,</i>	
12	593 F. Supp. 2d 876 (E.D. Va. 2009).....	7, 10
13	<i>Microsoft Corp. v. Sellers,</i>	
14	411 F. Supp. 2d 913 (E.D. Tenn. 2006)	7, 9
15	<i>Microsoft Corp. v. Silver Star Micro, Inc.,</i>	
16	2008 U.S. Dist. LEXIS 1526 (N.D. Ga. Jan. 9, 2008)	7
17	<i>Miller v. Yokohama Tire Corp.,</i>	
18	358 F.3d 616 (9th Cir. Cal. 2004)	10
19	<i>Monterey Bay Military Hous., LLC v. Pinnacle Monterey LLC,</i>	
20	116 F. Supp. 3d 1010 (N.D. Cal. 2015)	20
21	<i>Neder v. United States,</i>	
22	527 U.S. 1 (1999)	23
23	<i>Nsi Tech. Servs. Corp. v. NASA,</i>	
24	1996 U.S. Dist. LEXIS 22455 (N.D. Cal. May 13, 1996)	19
25	<i>Oracle Am., Inc. v. Service Key, LLC,</i>	
26	2012 WL 6019580 (N.D. Cal. Dec. 3, 2012)	24
27	<i>Oracle Am., Inc. v. TERiX Computer Co.,</i>	
28	2014 U.S. Dist. LEXIS 561 (N.D. Cal. Jan. 3, 2014)	13
	<i>Parks Sch. of Bus., Inc. v. Symington,</i>	
	51 F.3d 1480 (9th Cir. 1995).....	2
	<i>Peter Rosenbaum Photography Corp. v. Otto Doosan Mail Order, Ltd.,</i>	
	2005 U.S. Dist. LEXIS 21528 (N.D. Ill. Sept. 26, 2005).....	15
	<i>Platt Elec. Supply, Inc. v. EOFF Elec., Inc.,</i>	
	522 F.3d 1049 (9th Cir. 2008).....	21

1	<i>Platt v. Union Pac. R.R. Co.,</i>	
2	99 U.S. 48 (1878)	6
3	<i>PQ Labs, Inc. v. Qi,</i>	
4	2014 U.S. Dist. LEXIS 11769 (N.D. Cal. Jan. 29, 2014)	6
5	<i>Religious Tech. Ctr. v. Wollersheim,</i>	
6	971 F.2d 364 (9th Cir. 1992).....	18
7	<i>Schmuck v. United States,</i>	
8	489 U.S. 705 (1989)	16, 17
9	<i>Semegen v. Weidner,</i>	
10	780 F.2d 727 (9th Cir. 1985).....	21
11	<i>State Analysis, Inc. v. Am. Fin. Servs. Assoc.,</i>	
12	621 F. Supp. 2d 309 (E.D. Va. 2009).....	13
13	<i>Steward v. West,</i>	
14	2013 U.S. Dist. LEXIS 194238 (C.D. Cal. Sept. 6, 2013).....	15
15	<i>Stewart v. Wachowski,</i>	
16	2005 WL 6184235 (C.D. Cal. June 14, 2005)	14, 15
17	<i>Sussex Fin. Enters., Inc. v. Bayerische Hypo-und Vereinsbank,</i>	
18	2010 WL 94272 (N.D. Cal. Jan. 6, 2010)	24
19	<i>Synapsis, LLC v. Evergreen Data Systems, Inc.,</i>	
20	2006 WL 44239 (N.D. Cal. Jan. 9, 2006)	23
21	<i>Tabas v. Tabas,</i>	
22	47 F.3d 1280 (3d Cir. 1995).....	19
23	<i>United Energy Owners Comm., Inc. v. United States Energy Mgmt. Sys., Inc.,</i>	
24	837 F.2d 356 (9th Cir. 1988).....	20
25	<i>United States v. Abozid,</i>	
26	257 F.3d 191 (2d Cir. 2001).....	12
27	<i>United States v. Akram,</i>	
28	165 F.3d 452 (6th Cir. 1999).....	8
	<i>United States v. Bailey,</i>	
	41 F.3d 413 (9th Cir. 1994).....	12, 13
	<i>United States v. Bao,</i>	
	189 F.3d 860 (9th Cir. 1999).....	8
	<i>United States v. Beydoun,</i>	
	469 F.3d 102 (5th Cir. 2006).....	8

1	<i>United States v. Bily,</i>	
2	406 F. Supp. 726 (E.D. Pa. 1975)	15
3	<i>United States v. Blinder,</i>	
4	10 F.3d 1468 (9th Cir. 1993).....	20
5	<i>United States v. Brewer,</i>	
6	835 F.2d 550 (5th Cir. 1987).....	12
7	<i>United States v. Cusino,</i>	
8	694 F.2d 185 (9th Cir. 1982).....	16
9	<i>United States v. Feldman,</i>	
10	853 F.2d 648 (9th Cir. 1988).....	19
11	<i>United States v. Garlick,</i>	
12	240 F.3d 789 (9th Cir. 2001).....	16
13	<i>United States v. Garner,</i>	
14	663 F.2d 834 (9th Cir. 1981).....	16
15	<i>United States v. Green,</i>	
16	745 F.2d 1205 (9th Cir. 1985), <i>cert. denied</i> , 474 U.S. 925 (1985).....	16
17	<i>United States v. Handy,</i>	
18	761 F.2d 1279 (9th Cir. 1985).....	6
19	<i>United States v. Harrison,</i>	
20	534 F.3d 1371 (11th Cir. 2008).....	7
21	<i>United States v. Kirk,</i>	
22	844 F.2d 660 (9th Cir. 1988).....	19
23	<i>United States v. Liu,</i>	
24	731 F.3d 982 (9th Cir. 2013).....	14
25	<i>United States v. Lo,</i>	
26	231 F.3d 471 (9th Cir. 2000).....	16
27	<i>United States v. Lothian,</i>	
28	976 F.2d 1257 (9th Cir. 1992).....	17
	<i>United States v. Pelisamen,</i>	
	641 F.3d 399 (9th Cir. 2011).....	16
	<i>United States v. Petersen,</i>	
	98 F.3d 502 (9th Cir. 1996).....	12
	<i>United States v. Philip Morris USA Inc.,</i>	
	566 F.3d 1095 (D.C. Cir. 2009)	18

1	<i>United States v. Sepulveda</i> ,	
2	115 F.3d 882 (11th Cir. 1997).....	12
3	<i>United States v. Shipsey</i> ,	
4	363 F.3d 962 (9th Cir. 2004).....	17
5	<i>United States v. Thian Teh</i> ,	
6	535 F.3d 511 (6th Cir. 2008).....	8
7	<i>Vernor v. Autodesk, Inc.</i> ,	
8	621 F.3d 1102 (9th Cir. 2010).....	6
9	<i>Wang v. Rodriguez</i> ,	
10	830 F.3d 958 (9th Cir. 2016).....	9
11	<i>Ward v. Nat'l Entm't Collectibles Ass'n</i> ,	
12	2012 WL 12885073 (C.D. Cal. Oct. 29, 2012)	25
13	<i>Webster v. Omnitrition Int'l, Inc.</i> ,	
14	79 F.3d 776 (9th Cir. 1996).....	20
15	<i>Wilkins v. Gill</i> ,	
16	2017 U.S. Dist. LEXIS 57711 (S.D. Cal. Apr. 14, 2017)	2
17	Statutes	
18	17 U.S.C. § 506.....	10, 14
19	17 U.S.C. § 1201	4, 5, 6
20	18 U.S.C. § 1029	10, 11, 12
21	18 U.S.C. § 1343	10, 16
22	18 U.S.C. § 1961	10
23	18 U.S.C. § 1962	21
24	18 U.S.C. § 2318.....	<i>passim</i>
25	18 U.S.C. § 2319.....	14, 15
26	18 U.S.C. § 2320	5, 8, 9
27	18 U.S.C. § 2320.....	8
28	Cal. Civ. Code § 1710.....	24

INTRODUCTION

Synopsys is a world leader in semiconductor design software, founded in the Bay Area and headquartered in Mountain View, California. In the fall of 2013, Defendants Ubiquiti Networks, Inc. (“Ubiquiti”), Ubiquiti Networks International Limited (“UNIL”), Ching-Han Tsai, and unknown Does operating in the U.S. and Taiwan agreed on a scheme to pirate Synopsys’ high-value software in order to reduce Ubiquiti and UNIL’s semiconductor design costs and reap illegal profits at Synopsys’ expense. Over the course of the next nearly three years, Defendants relentlessly pirated thirteen separate Synopsys software applications, violating a multitude of federal criminal statutes along the way. Among other illegal activities, Defendants willfully created and distributed unauthorized copies of Synopsys’ software, forged counterfeit electronic license keys to circumvent Synopsys’ technical measures to protect its software, and continually lied to Synopsys in order to obtain and maintain access to Synopsys’ file download and customer support websites. All told, Defendants used counterfeit license keys to access Synopsys’ software over 39,000 times before Synopsys discovered their activity and issued a cease and desist demand in May 2016. Even after Synopsys’ May 2016 cease and desist, Defendants accessed Synopsys’ software using counterfeit license keys. The value of Defendants’ use of Synopsys’ software and statutory damages for Defendants’ violations of law total tens of millions of dollars.

Defendants’ motion to dismiss advances a slew of superficial arguments, most of which relate to the central theme that Defendants cannot be liable for any software-piracy “trafficking” related offenses because Tsai, Ubiquiti, and UNIL comprise a single corporate unit. *See* Dkt. 34 (Motion) at 5, 7, 12-13, & 22. This fundamental pillar of Defendants’ motion misapprehends the scope of governing statutes, ignores Synopsys’ allegations that Defendants created, distributed, and imported circumvention technology, and is belied by UNIL’s Rule 12(b)(2) motion.¹ One other reoccurring theme emerges from Defendants’ motion. Throughout their brief, Defendants carefully avoid discussing the First Amended Complaint’s (“FAC”) detailed factual allegations and adverse case law that contradict Defendants’ arguments. This tactic evinces the hollowness

¹ UNIL’s Rule 12(b)(2) avers that Ubiquiti and UNIL “observe all corporate formalities maintaining their separate existence.” Dkt. 35 (UNIL Motion to Dismiss) at 6:19-20.

of Defendants' motion. Fulsome analysis of the FAC and the law establishes that Defendants' motion to dismiss should be denied in its entirety.

LEGAL STANDARD

A court may dismiss a complaint under Rule 12(b)(6) when it does not contain enough facts to state a plausible claim for relief. *GreenCycle Paint, Inc. v. PaintCare, Inc.*, 2017 U.S. Dist. LEXIS 55314, at *9-10 (N.D. Cal. Apr. 11, 2017) (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* In assessing a Rule 12(b)(6) motion, "the Court must accept as true all material allegations in the complaint, as well as reasonable inferences to be drawn from them, and must construe the FAC in the light most favorable to the plaintiff." *E.g., Wilkens v. Gill*, 2017 U.S. Dist. LEXIS 57711, at *6 (S.D. Cal. Apr. 14, 2017) (citing *Parks Sch. of Bus., Inc. v. Symington*, 51 F.3d 1480, 1484 (9th Cir. 1995) and *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)).

FACTUAL BACKGROUND

Synopsys develops and owns copyrights to a comprehensive, integrated portfolio of software that helps companies design, test, and manufacture semiconductors. FAC at ¶¶ 22-24. As the fifteenth largest software company in the world, Synopsys' broad range of software is highly valuable, and many companies seek Synopsys' solutions to aid their businesses. FAC ¶ 23. Synopsys does not sell ownership rights to its software. FAC ¶ 25. Rather, Synopsys' customers purchase licenses that grant them limited rights to install and use Synopsys software on particular computers at particular locations. FAC ¶ 25. Synopsys takes protection of its copyrighted software seriously. In order to protect its valuable software from piracy, Synopsys developed a License Key System that controls access to its software. FAC ¶ 26. Synopsys' License Key System requires users to access a license key code in order to execute Synopsys software applications, and validation of the user's license key establishes the quantity and term of the licensed software in accordance with the license terms. FAC ¶ 26.

Ubiquiti is a Delaware corporation with its principal place of business in San Jose, California. FAC ¶ 2. Ubiquiti and its wholly owned subsidiaries develop networking technology

1 for service providers and enterprises. FAC ¶ 3. Some of Ubiquiti's research and development
 2 operations are conducted at facilities outside the U.S., including in Taiwan. FAC ¶¶ 3-5. One of
 3 Ubiquiti's offshore R&D facilities is UNIL's Taiwan branch office in Taipei. FAC ¶¶ 6, 8.

4 UNIL is an entity incorporated under the laws of Hong Kong. According to UNIL's Rule
 5 7.1 disclosure statement, UNIL's parent company is Ubiquiti Holding Company Limited, a
 6 Cayman Islands entity. *See* Dkt. 26. UNIL's disclosure statement states that Ubiquiti is UNIL's
 7 "grandparent company," but that Ubiquiti owns less than 10% of UNIL's stock. *Id.*

8 From October 2013 to present, Defendant Tsai has worked for Ubiquiti in Taipei and San
 9 Jose, FAC ¶¶ 12-13, apparently managing the semiconductor design team responsible for the
 10 federal crimes alleged in the FAC. Sometime prior to October 2013, Tsai and others at Ubiquiti
 11 and UNIL conspired to, and did, form an associated-in-fact enterprise ("Piracy Enterprise") with a
 12 common purpose of pirating Synopsys' software in order to lower Ubiquiti's and UNIL's
 13 semiconductor development costs and reap ill-gotten profits. FAC ¶ 29. The Piracy Enterprise's
 14 objectives included fraudulently obtaining Synopsys' software, making unauthorized copies of it,
 15 and using counterfeit license keys to circumvent Synopsys' License Key System. *Id.*

16 In furtherance of Defendants' conspiracy, between September 2013 and May 2014, Tsai
 17 and others acting on behalf of Ubiquiti and UNIL used the pretext of good faith licensing
 18 discussions to fraudulently induce Synopsys into granting Defendants access to Synopsys'
 19 software. FAC ¶¶ 35-41, 46. Based on Defendants' numerous fraudulent statements, Synopsys
 20 executed a limited 90-day evaluation license agreement with Ubiquiti and created a user account
 21 giving Ubiquiti access to Synopsys' customer support and download websites. FAC ¶¶ 43, 44.
 22 Unbeknownst to Synopsys, as soon as they obtained access to Synopsys' file download and
 23 customer support websites, Defendants began making and distributing unauthorized copies of
 24 Synopsys' software and documentation. FAC ¶¶ 42, 51. Defendants then used tools obtained
 25 from hacker websites to create counterfeit license keys to circumvent Synopsys' software
 26 protection systems. FAC ¶¶ 28, 63. Ubiquiti, UNIL, and other members of the Piracy Enterprise
 27 used these tools to create counterfeit license keys for 13 separate Synopsys software applications,
 28 which Defendants distributed to various employees of Ubiquiti and UNIL in California and

Taiwan. FAC ¶¶ 63, 66, 88-89, 97-98, 100-101, 104. Defendants secretly used counterfeit license keys to circumvent Synopsys' License Key System and pirate Synopsys software over 39,000 times. FAC ¶¶ 28, 32, 65. Defendants distributed counterfeit license keys and key generation tools from corporation to corporation using the Internet and shared communications networks, all the while taking steps to obfuscate and alter Host IDs, IP addresses, and MAC addresses for the computers using the pirated software applications. FAC ¶¶ 58-64; 133.

Synopsys discovered Defendants' illegal conduct and demanded that they cease and desist its unauthorized use of Synopsys' software in May 2016. FAC ¶ 65. In defiance of the cease and desist letter, and in furtherance of their fraudulent and criminal scheme, the Defendants continued to access Synopsys' software using counterfeit keys after receipt of Synopsys' cease and desist demand. FAC ¶ 65.

ARGUMENT

I. SYNOPSYS PROPERLY ALLEGES ALL OF ITS DMCA CLAIMS

The Digital Millennium Copyright Act ("DMCA") prohibits use and trafficking of technology designed to circumvent technological measures that prevent access to, or infringement of, copyrighted works. Defendants do not dispute that the counterfeit and illicit license keys they used to access Synopsys' software qualify as circumvention technology for purposes of 17 U.S.C. § 1201(a)(1).² Thus, the only questions presented are whether the FAC alleges that Defendants "manufactured, imported, offered to the public, provided, or otherwise trafficked" counterfeit and illicit license keys under section 1201(a)(2) and 1201(b), and whether Synopsys' License Key System protects any of Synopsys' copyright rights as required by section 1201(b).

A. The FAC States Many Violations of DMCA Sections 1201(a)(2) and 1201(b)

Section 1201(a)(2) provides in pertinent part: "No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that...is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access" to a copyright protected work. Section 1201(b) similarly provides that no person "shall manufacture, import, offer to the public, provide,

² Defendants do not seek dismissal of Synopsys' claim under 17 U.S.C. § 1201(a)(1).

1 or otherwise traffic in any technology...that effectively protects a right of a copyright owner.”
 2 Here, the FAC alleges that Defendants *manufactured* circumvention technology by creating
 3 counterfeit license keys (*e.g.*, FAC ¶¶ 28, 33, 51, 57, 58),³ *imported* circumvention technology by
 4 transmitting circumvention technology from Taiwan to the United States, (*e.g.*, FAC ¶¶ 42, 58,
 5 56, 59, 66, 80), *provided* circumvention technology to one another over shared networks for
 6 commercial purposes, (*id.*, *see also* FAC ¶¶ 60-63), and *otherwise trafficked* in circumvention
 7 technology by distributing such technology from corporation to corporation in furtherance of
 8 commercial objectives (*see, e.g., id.* and FAC ¶¶ 8, 9, 12).

9 Defendants’ argument that their conduct was not “sufficiently public” to constitute
 10 “trafficking” because they did not make counterfeit keys and counterfeiting tools available to
 11 “others” or “third parties” fails for three reasons. Dkt. 34 at 5:12-13. First, Defendants’ argument
 12 altogether ignores the FAC’s allegations that Defendants manufactured and imported
 13 circumvention technology; these allegations are sufficient in and of themselves to state section
 14 1201(a)(2) and section 1201(b) claims under the plain text of the statutes.⁴ Second, the FAC *does*
 15 allege that each Defendant provided circumvention technology to one or more third parties,
 16 including at least to each other. Defendants’ cited authorities are unavailing. Unlike the FAC,
 17 which alleges Defendants created, imported, and distributed circumvention technology between
 18 distinct corporate entities, *Ass’n for Info. Media & Equip. v. Regents of the Univ. of Cal.* involved
 19 a single school’s use of off-the-shelf video editing software that didn’t even qualify as
 20 circumvention technology in the first place. 2012 WL 7683452, at *9 (C.D. Cal. Nov. 20, 2012).⁵
 21 The other cases Defendants cite simply state the general requirement of third party access, which

22 ³ Relying on an incomplete quotation of FAC ¶ 28, Defendants argue that the FAC only alleges
 23 that Defendants “patronized websites that traffic in [counterfeit] keys,” and that Defendants are
 24 mere “end users.” Dkt. 34 at 4:26-5:3. But Defendants’ quotation omits the portion of FAC ¶ 28
 that alleges that Defendants *created* counterfeit keys using *tools* obtained from hacker websites.

25 ⁴ *A fortiori*, if unilateral actions like creating, transporting, importing, and exporting amount to
 trafficking under 18 U.S.C. § 2318 and 18 U.S.C. § 2320, *see* Sections II and III(A), *infra*, such
 26 unilateral actions amount to trafficking under the DMCA.

27 ⁵ The FAC in *Ass’n for Info. Media & Equip. v. Regents of the Univ. of Cal.* did not allege that the
 school *provided* circumvention technology to third parties, it alleged only that the school “on a
 28 direct and/or contributory and/or vicarious basis” “allowed” or “sanctioned” trafficking by others
 in circumvention technology. No. 2:10-cv-09378-CBM-MAN, Dkt. No. 21-5 (C.D. Cal. Feb. 15,
 2011)

1 the FAC satisfies by alleging that the Defendants distributed keys among two distinct corporate
 2 entities. No case supports Defendants' illusory requirement that the third party receiving the
 3 circumvention technology be "unaffiliated" (whatever that means) with the entity that created or
 4 provided the circumvention technology at issue. Dkt. 34 at 6:3-4.

5 Third, Defendants' argument conflates the term "provide" with the term "traffic." Dkt. 34
 6 at 5:8-18 & fn. 1. But these terms presumptively mean different things. *E.g.*, *Ctr. for Biological*
 7 *Diversity v. Salazar*, 695 F.3d 893, 903 (9th Cir. 2012); *Platt v. Union Pac. R.R. Co.*, 99 U.S. 48,
 8 58 (1878) ("rules of statutory construction declare that a legislature is presumed to have used no
 9 superfluous words. Courts are to accord a meaning, if possible, to every word in a statute.");
 10 *Duncan v. Walker*, 533 U.S. 167, 174 (2001) (rejecting the Government's construction of a statute
 11 that would render one word "insignificant, if not wholly superfluous"); *United States v. Handy*,
 12 761 F.2d 1279, 1280 (9th Cir. 1985) (similar). Defendants' argument renders the term "provide"
 13 superfluous. In any event, the FAC alleges multiple acts that constitute trafficking under any
 14 conception of that term, *see* Sections II and III(A), *infra*, so the Court need not strike new ground
 15 by adjudicating Defendants' argument about the meaning of the term "provide."

16 **B. Synopsys' License Key System Protects its Reproduction Right**

17 Section 1201(b) prevents circumvention of technological measures that "effectively
 18 protect[] a right of a copyright owner." Here, the FAC alleges that Synopsys' License Key
 19 System protects Synopsys' reproduction right. "In order to use a software program, a user's
 20 computer will automatically copy the software into the computer's random access memory
 21 ('RAM'), which is a form of computer data storage." *Vernor v. Autodesk, Inc.*, 621 F.3d 1102,
 22 1109 (9th Cir. 2010). Unauthorized copying of software into RAM at runtime "creates a 'copy'
 23 of that software in violation of the Copyright Act." *PQ Labs, Inc. v. Qi*, 2014 U.S. Dist. LEXIS
 24 11769, at *18-19 (N.D. Cal. Jan. 29, 2014) (citing *MAI Sys. Corp. v. Peak Computer, Inc.*, 991
 25 F.2d 511, 518-19 (9th Cir. 1993)). By preventing execution of Synopsys' software without a
 26 valid license key (FAC ¶ 26), Synopsys' License Key System prevents copying of its software to
 27 RAM on computers where such copies are not authorized. *Airframe Systems, Inc. v. Raytheon*
 28 *Co.*, 520 F. Supp. 2d 258, 267 (D. Mass. 2007) ("[w]ith regard to software, an act of copying

sufficient to violate the Copyright Act occurs each time the software is run.”).

II. SYNOPSIS PROPERLY ALLEGES THAT DEFENDANTS TRAFFICKED COUNTERFEIT AND ILLICIT LABELS

Among other wrongful acts, 18 U.S.C. § 2318 prohibits trafficking of counterfeit and illicit “labels” accompanying computer programs, which the statute defines to include labeling components used by copyright owners to identify copies of computer programs and to verify that a copy of a computer program is not counterfeit or infringing. A counterfeit label is a non-genuine article, whereas an illicit label is a genuine article misused in one of two statutorily prohibited manners. *Microsoft Corp. v. Pronet Cyber Techs., Inc.*, 593 F. Supp. 2d 876, 886 (E.D. Va. 2009). The FAC states claims against each Defendant for trafficking in both counterfeit labels (counterfeit license keys) and illicit labels (valid but misused temporary keys).

It is well settled that software authentication keys such as the Synopsys license keys at issue in this case qualify as “identifying labels” for purposes of section 2318. *Id.* at 878-79 (holding that “Product Keys, which are 25-character alphanumeric codes, unique to each licensee to whom a product is distributed, that must be entered by a user in order for the Microsoft program to operate properly” are identifying labels under section 2318); *Microsoft Corp. v. EEE Bus., Inc.*, 555 F. Supp. 2d 1051, 1059 (N.D. Cal. 2008) (same, noting that form of product key identified software as a “volume license” product).⁶ Defendants completely ignore this well-established body of case law and the plain text of section 2318 in order to advance a scattershot of meritless arguments.

“Trafficking.” The broad statutory definition of “trafficking” under section 2318 (which Defendants attempt to gloss over in a footnote) defines “trafficking” to mean “to *transport*,

⁶ See also *United States v. Harrison*, 534 F.3d 1371, 1373 (11th Cir. 2008) (same); *Microsoft Corp. v. Buy More, Inc.*, 136 F. Supp. 3d 1148, 1157 (C.D. Cal. 2015) (same); *Microsoft Corp. v. AGA Solutions, Inc.*, 2010 U.S. Dist. LEXIS 26756, at *6 (E.D.N.Y. Mar. 22, 2010) (same); *Microsoft Corp. v. Ion Techs. Corp.*, 484 F. Supp. 2d 955, 959 (D. Minn. 2007) (same); *Microsoft Corp. v. # 9 Software, Inc.*, 2005 U.S. Dist. LEXIS 36710, at *2 (E.D. Va. Dec. 15, 2005) (same); *Microsoft Corp. v. Sellers*, 411 F. Supp. 2d 913, 917 & n.3 (E.D. Tenn. 2006) (same); *Microsoft Corp. v. A Plus Open LLC*, 2007 U.S. Dist. LEXIS 8435, at *1 (D. Colo. Feb. 6, 2007) (same); *Microsoft Corp. v. Silver Star Micro, Inc.*, 2008 U.S. Dist. LEXIS 1526, at *2-3 (N.D. Ga. Jan. 9, 2008) (same).

1 *transfer, or otherwise dispose of, to another, for purposes of commercial advantage or private*
 2 *financial gain, or to make, import, export, obtain control of, or possess, with the intent to so*
 3 *transport, transfer, or otherwise dispose of.”* 18 U.S.C. § 2320(f)(5) (emphasis added). Here, the
 4 FAC alleges that Defendants, for commercial purposes and private gain (FAC ¶ 29), committed
 5 multiple independent acts that each constitute trafficking under section 2320’s definition,
 6 including making counterfeit license keys, transporting counterfeit keys over the Internet,
 7 transferring counterfeit and illicit license keys between distinct corporate entities, and importing
 8 and exporting counterfeit and illicit license keys. *E.g.*, FAC ¶¶ 8, 9, 12, 28, 33, 42, 51, 57, 58-63.
 9 These allegations are sufficient to establish Synopsys’ claims under section 2318.

10 “Trafficking” under section 2318 does not require that Defendants “sold or offered to sell
 11 license keys,” or that Defendants be “in the business of selling” license keys, as Defendants
 12 suggest. Dkt. 34 at 7:7-12; *see, e.g., United States v. Beydown*, 469 F.3d 102, 105 (5th Cir. 2006)
 13 (defendant could be liable for trafficking “even if [he] never sold a single infringing booklet”).
 14 Nor does the statute require the involvement of “others” to establish trafficking. Dkt. 34 at 7:7-
 15 12. In fact, several “trafficking” crimes identified in section 2320 (including the acts of creating,
 16 transporting, importing, and exporting at issue here) can be completed without the involvement of
 17 any third party at all. *See, e.g., Beydown*, 469 F.3d at 105 (violation of section 2318 was complete
 18 after defendant made counterfeit labels).⁷ In any event, the FAC *does* allege that each Defendant
 19 transferred counterfeit and illicit keys to “others”: *inter alia*, Ubiquiti transferred illicit keys to
 20 UNIL, and UNIL transferred counterfeit keys to Ubiquiti. The fact that Defendants may have
 21 only trafficked such keys to other co-conspirators does not absolve them of liability. *See United*
 22 *States v. Bao*, 189 F.3d 860, 863 (9th Cir. 1999) (affirming section 2318 conviction based on
 23 defendants sale of counterfeit documentation to co-conspirators); *United States v. Thian Teh*, 535
 24 F.3d 511, 520 (6th Cir. 2008) (affirming section 2318 conviction based on defendant’s unilateral
 25 importation of counterfeit DVD labels).

26
 27 ⁷ *See also United States v. Akram*, 165 F.3d 452, 454 (6th Cir. 1999) (affirming section 2318
 28 conviction based solely on the fact that defendant was found driving on interstate highway in a U-
 Haul truck that contained counterfeit goods); *Ion Techs. Corp.*, 484 F. Supp. 2d at 961 (finding
 independent basis for liability based solely on act of shipping illicit labels).

1 **“Accompanying.”** Defendants are incorrect to assert that Synopsys’ license keys are not
 2 “part of the software package” it delivers to customers simply because Synopsys sometimes
 3 transmits license keys in a standalone email. Dkt. 34 at 8:1-7. The fact that Synopsys’ license
 4 keys are not physically “attached” to a user’s software download is of no moment, because
 5 section 2318 prohibits trafficking in labels that are “affixed to, enclosing, *or accompanying*” a
 6 copy of a computer program. Defendants’ argument reads the disjunctive phrase “or
 7 accompanying” out of section 2318 by requiring the subject label to be digitally “affixed to” or
 8 “enclosing” the software. Not only does Defendants’ argument ignore the text of section 2318, it
 9 ignores the modern reality of digital distribution. It is common for software and digital service
 10 providers to send separate emails containing passwords needed to access electronic downloads or
 11 services. Synopsys’ license keys are undoubtedly “part of the software package” delivered to
 12 customers. *Every* authorized copy of Synopsys’ software *must* be accompanied by a license key
 13 in order to authenticate the copy that a specific user is entitled to run. FAC ¶¶ 25, 26.

14 **Genuine Appearance.** Defendants’ argument that the FAC does not allege that the
 15 counterfeit license keys they used “appeared to be genuine” is contrary to the allegations of the
 16 FAC. FAC at ¶ 99 (genuine appearance); ¶ 28 (counterfeit keys enabled access to Synopsys
 17 software). Defendants’ argument that “trafficking” under section 2318 requires “that the
 18 Defendants palmed [license keys] off to third parties under [the false] pretense” of authenticity is
 19 also incorrect. Dkt. 34 at 8:12-14. Persons can be liable for trafficking counterfeit articles “even
 20 though the direct buyer knows the goods are knock-offs.” *See, e.g., Wang v. Rodriguez*, 830 F.3d
 21 958, 962 (9th Cir. 2016) (collecting cases and interpreting 18 U.S.C. § 2320). In fact, much of the
 22 case law applying section 2318 in the software context involves distribution of inherently illegal
 23 standalone product keys to recipients who knew the product keys were not genuine. *See # 9*
 24 *Software, Inc.*, 2005 U.S. Dist. LEXIS 36710, at *2; *Sellers*, 411 F. Supp. 2d at 917 & n.3; *A Plus*
 25 *Open LLC*, 2007 U.S. Dist. LEXIS 8435, at *1.⁸

26
 27 ⁸ To the extent the Court accepts any of Defendants’ arguments, Synopsys can amend its FAC to
 28 allege that (1) Synopsys sent to Tsai a single delivery email containing links to download VCS
 and a license key for VCS; (2) Synopsys’ license keys are comprised of human readable
 alphanumeric text elements that identify which version and features of Synopsys products have
 been licensed for use in connection with a particular user’s copy of software; and (3) that the

Illicit Labels. Defendants’ motion to dismiss Synopsys’ illicit label trafficking claim is based on two false premises. First, Defendants’ argument that Synopsys license keys “control Synopsys’ distribution channel and nothing more” (Dkt. 34 at 8:26-27) is incorrect, as the FAC alleges that Synopsys’ license keys prevent unauthorized execution (and copying) of its software, and that the keys help Synopsys identify infringing use of its software. Defendants’ citation to *Ion Techs* (Dkt. 34 at 9:9-12) actually defeats their own argument, as the illicit labels in that case (Microsoft Windows Certificates of Authenticity) contained alphanumeric product keys designed to serve the same fundamental purpose as Synopsys’ license keys. *See, e.g., Pronet Cyber Techs.*, 593 F. Supp. 2d at 878 (“the Product Key for a particular copy of a program is located on the unique [Certificate of Authenticity]...By maintaining an internal list [of Product Keys]...Microsoft is able to determine whether a given user has the appropriate license for the product in that user's possession.”).

Second, Defendants’ argument is based on the false assertion that Defendants only used temporary license keys in connection with the specific software copies for which they were intended, *i.e.*, the software binary files “downloaded by Defendants from Synopsys’ website with Synopsys authorization.” Dkt. 34 at 8:27-28. But the FAC alleges that Defendants made *unauthorized* copies of Synopsys’ software and then improperly used *someone else’s* legitimate temporary key to access those unauthorized copies. FAC ¶ 37, 39, 51, 59. These allegations state a claim for trafficking in illicit labels. *See, e.g., Pronet Cyber Techs.*, 593 F. Supp. 2d at 878.

III. SYNOPSYS ALLEGES RICO CLAIMS AGAINST ALL DEFENDANTS

“Liability [for civil RICO violations] requires (1) the conduct (2) of an enterprise (3) through a pattern (4) of racketeering activity.” *Miller v. Yokohama Tire Corp.*, 358 F.3d 616, 620 (9th Cir. Cal. 2004) (citations omitted). “Racketeering activity” is defined in 18 U.S.C. § 1961(1)(B) to include a number of federal crimes, including trafficking in counterfeit or illicit software labels (18 U.S.C. § 2318), trafficking in counterfeit access devices (18 U.S.C. § 1029); criminal copyright infringement (17 U.S.C. § 506), and wire fraud (18 U.S.C. § 1343).

counterfeit keys used by Defendants mimicked the human readable text and format of Synopsys’ genuine keys, including text indicating that Synopsys is the “issuer” of the keys, and would thus appear to an innocent reader of the key file to be a genuine Synopsys license key.

Here, the FAC alleges that Ubiquiti, UNIL, and Tsai formed a conspiracy in or about October 2013 pursuant to which they agreed to pirate Synopsys' software through a series of criminal acts. FAC ¶ 29.⁹ The FAC further alleges that Ubiquiti, UNIL, and Tsai carried out their conspiracy from at least October 2013 to June 2016 through a pattern of conducting Ubiquiti and UNIL's affairs via criminal conduct, i.e., making, distributing, and using counterfeit labels, counterfeit access devices, and illegal copies of Synopsys' software in order to lower Ubiquiti and UNIL's development costs and reap illegal profits at Synopsys' expense. The FAC also provides specific details about the dates on which numerous predicate acts occurred. These allegations establish a RICO claim.

A. The FAC Alleges Counterfeit Access Device Use and Trafficking

Section 1029 generally prohibits possession, use, and trafficking of counterfeit access devices and counterfeit access device making tools. Section 1029(e)(1) broadly defines "access device" to mean:

any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)

(emphasis added).

Covered Access Devices. Relying on an incomplete snippet of legislative history, Defendants argue that their use of counterfeit and illicit electronic license keys to access Synopsys software did not violate section 18 U.S.C. § 1029 because it is "a statute aimed at credit card fraud." Dkt. 34 at 11:3-4. But Defendants ignore a wealth of adverse legislative history and case law that is directly contrary to their position. "Both the Senate and House Reports on the

⁹ Defendants feign confusion at the FAC's allegation that Tsai agreed with "others at Ubiquiti and UNIL," which Defendants say makes them unsure about whether Ubiquiti and UNIL are members of the alleged Piracy Enterprise. This argument is baseless. It is axiomatic that corporations act through their employees, and the FAC unequivocally alleges that Ubiquiti and UNIL were part of the Piracy Enterprise. *See, e.g.*, FAC ¶¶ 29 (alleging "Tsai, Ubiquiti, and UNIL each took wrongful acts in furtherance of *their* unlawful agreement")(emphasis added); 31 ("Tsai, Ubiquiti, and UNIL have each used the Internet...in the course of conducting the Piracy Enterprise"); 126 ("Tsai, Ubiquiti, and UNIL have conducted...the Piracy Enterprise"); 127 ("Tsai, Ubiquiti, and UNIL conspired...").

1 statute state that the definition of ‘access device’ was intended to be ‘broad enough to encompass
 2 technological advances.’” *United States v. Brewer*, 835 F.2d 550, 553 (5th Cir. 1987). Consistent
 3 with this legislative intent, courts have found a wide range of items to fit the definition of “access
 4 devices,” including modified mobile phones, *United States v. Sepulveda*, 115 F.3d 882, 884 (11th
 5 Cir. 1997), airline tickets, *United States v. Abozid*, 257 F.3d 191, 193 (2d Cir. 2001), microchips
 6 with embedded tumbling software, *United States v. Bailey*, 41 F.3d 413, 418 (9th Cir. 1994), and
 7 even computer passwords, *United States v. Petersen*, 98 F.3d 502, 505 (9th Cir. 1996).

8 The FAC alleges two types of access devices: counterfeit license keys and virtual
 9 machines configured by Defendants to use counterfeit and illicit license keys. Defendants do not
 10 seriously dispute that electronic license keys can constitute access devices, and for good reason.
 11 See *Bailey*, 41 F.3d at 418 (“access device” included software designed to circumvent telephone
 12 companies’ system for access control); *Petersen*, 98 F.3d at 505 (“access device” included
 13 computer passwords that gave hacker access to bank’s network). The virtual machines
 14 Defendants configured for the specific purpose of using counterfeit license keys to bypass
 15 Synopsys security measures also constitute access devices. *United States v. Sepulveda*, cited by
 16 Defendants, does not stand for the proposition that a computer can never constitute an access
 17 device.¹⁰ On the contrary, *Sepulveda* held that specially programmed “clone” cell phones
 18 designed to trick phone providers’ systems into associating the clone cell phones with valid ESN-
 19 MIN combination codes constituted “access devices.” 115 F.3d at 886. Like the cloned cell
 20 phones in *Sepulveda* designed to broadcast apparently legitimate ESN-MINs in order to trick the
 21 phone networks into granting the cloned phones access to the telephone routing system, the
 22 virtual machines Defendants used were designed to broadcast false license account information in
 23 order to trick Synopsys’ License Key System into granting access to Synopsys’ software.

24 **Account Access.** Defendants’ argument that the counterfeit access devices they used are
 25 not within reach of section 1029 because their use of such devices “did not create a ‘contractual
 26 relationship’ with Synopsys” (Dkt. 34 at 12:11-12) misapprehends Ninth Circuit law. In *United*

27 ¹⁰ The cited passage from *Sepulveda* discusses the *defendants’* argument that a general purpose
 28 computer defendants used to program cloned ESN-MID was not itself an access device. 115 F.3d
 at 888. No party in *Sepulveda* contended otherwise.

1 *States v. Bailey*, the Ninth Circuit held:

2 When the statute refers to “account access,” it evidently means access to the *privileges*
 3 *permitted by virtue of the maintenance of an account....*[A]ctual or potential recourse by
 4 the provider of the goods or services against the party for whose benefit the account is
 5 maintained is not a necessary element of “account access” under § 1029. *It matters only*
that the user of the access device be able to obtain goods or services from which he would
otherwise be excluded.

6 41 F.3d 413, 417-418 (9th Cir. 1994) (emphasis added). Here, the FAC alleges that in order to
 7 gain access to Synopsys’ software, end users must enter into a license agreement with Synopsys
 8 in order to obtain a user account that permits them to access Synopsys software. FAC ¶¶ 43-45.
 9 The FAC further alleges that Ubiquiti entered into an evaluation license agreement whereby it
 10 undertook to abide by Synopsys’ terms in exchange for creating a user account on Synopsys’
 11 download and customer support systems that allowed Ubiquiti to download and use Synopsys
 12 software and documentation. *Id.* Each and every time Defendants used a counterfeit key, they
 13 tricked Synopsys’ license key system into associating Defendants’ computers with a valid,
 14 licensed customer account and thereby gained “privileges permitted by virtue of the maintenance
 15 of an account” and access to “goods . . . from which [they] would otherwise be excluded.”
 16 *Bailey*, 41 F.3d at 417-18.

17 **Possession, Use, and Trafficking.** The FAC alleges Defendants used unauthorized
 18 access devices by using temporary keys that were not issued to them. FAC ¶¶ 56, 97, 98. The
 19 FAC alleges that Defendants possessed and used counterfeit access devices by using counterfeit
 20 license keys in order to access Synopsys software without paying for it. FAC ¶ 28. The FAC also
 21 alleges that Defendants created counterfeit access devices by making custom counterfeit keys. *Id.*
 22 Standing alone, these acts constitute cognizable predicate act violations under section 1029. In
 23 addition, the FAC also alleges that Defendants trafficked counterfeit access devices by importing,
 24 exporting, and transferring them from one corporation to another. Unlike the allegations in
 25 *Oracle Am., Inc. v. TERiX Computer Co.*, 2014 U.S. Dist. LEXIS 561, at *19 (N.D. Cal. Jan. 3,
 26 2014) and *State Analysis, Inc. v. Am. Fin. Servs. Assoc.*, 621 F. Supp. 2d 309, 317 (E.D. Va.
 27 2009), the FAC does not allege a claim against Defendants for “merely trafficking by receiving”
 28 license keys. *See Oracle*, 14 U.S. Dist. LEXIS 561, at *19. On the contrary, the FAC alleges that

each Defendant manufactured and *sent* counterfeit and unauthorized keys to a distinct corporate entity.

B. The FAC Alleges Criminal Copyright Infringement

Federal criminal statutes prohibit willful infringement of copyrights for purposes of commercial advantage and private financial gain. *See* 17 U.S.C. § 506; 18 U.S.C. § 2319. “Willfully” as used in § 506(a) “connotes a ‘voluntary, intentional violation of a known legal duty.’” *United States v. Liu*, 731 F.3d 982, 990 (9th Cir. 2013) (quoting *Cheek v. United States*, 498 U.S. 192, 201 (1991)). Synopsys has alleged that Defendants engaged in such conduct. *See* FAC ¶¶ 29, 42-43, 56, 65.

Synopsys has alleged that Synopsys is the owner of copyright protected software, FAC ¶ 24, and that after deceiving Synopsys into granting them access to Synopsys’ copyright protected software, Defendants knowingly began making, distributing, and using copies of Synopsys’ software without authorization in furtherance of a piracy scheme designed to lower Ubiquiti and UNIL’s semiconductor design costs and reap ill-gotten profits at Synopsys’ expense. FAC ¶¶ 42, 56, 65. The FAC further alleges the specific software copied as well as date ranges for when the illegal copying occurred. FAC ¶¶ 28, 29, 42, 45, 63. The FAC alleges that Defendants had knowledge of the unlawfulness of their conduct, *inter alia* because Ubiquiti entered into a license agreement expressly prohibiting unauthorized copying, FAC ¶ 43, and because Defendants continued to access unauthorized copies of Synopsys software even after receiving a cease and desist demand. FAC ¶ 65. Moreover, Defendants knew that they needed a license key to access Synopsys software, but rather than pay for that privilege, they decided to make counterfeit keys to access the unauthorized copies of Synopsys’ software that they made. The only plausible inference to draw from the FAC’s allegations of deception and use of counterfeit license keys is that Defendants knew what they were doing was illegal.

Defendants’ audacious argument that their copyright infringement was not “large-scale” enough to serve as a RICO predicate fails for two independent reasons. Dkt. 34 at 14:7-17 (citing *Stewart v. Wachowski*, 2005 WL 6184235, at *5 (C.D. Cal. June 14, 2005)). First, Synopsys respectfully submits that *Stewart v. Wachowski*, the case underlying Defendants’ argument, is

1 incorrect. In *Stewart*, despite finding the subject statutes to be “unambiguous on their face,” the
 2 district court relied on legislative history to conclude that 18 U.S.C. § 2319 only applies to
 3 unspecified “piracy or counterfeiting” offenses. *Id.* At least one district court has expressly
 4 rejected *Stewart’s* reasoning, *ICONICS, Inc. v. Massaro*, 192 F. Supp. 3d 254, 269 (D. Mass.
 5 2016) (rejecting *Stewart*), and *Stewart* is at odds with other district court cases finding allegations
 6 of willful copyright infringement sufficient to state criminal copyright violations, *see Bryant v.*
 7 *Mattel, Inc.*, 573 F. Supp. 2d 1254, 1269 (C.D. Cal. 2007); *Peter Rosenbaum Photography Corp.*
 8 *v. Otto Doosan Mail Order, Ltd.*, 2005 U.S. Dist. LEXIS 21528, *14 (N.D. Ill. Sept. 26, 2005).¹¹
 9 It is blackletter law that “plain text of the statute, not excursions through legislative history,
 10 governs” when there is no ambiguity. *ICONICS*, 192 F. Supp. 3d at 269; *accord H.J. Inc. v.*
 11 *Northwestern Bell Tel. Co.*, 492 U.S. 229, 245 (1989) (plain language governs in the context of
 12 RICO).

13 Second, assuming that *Stewart’s* holding is correct, it does not provide any brightline test
 14 or clear rule of decision foreclosing Synopsys’ criminal copyright claim against Defendants. On
 15 the contrary, the FAC fits neatly within the confines of the framework discussed in *Stewart*.
 16 Defendants’ infringement *was* “large-scale” and “enormously lucrative” software piracy of the
 17 type contemplated in *Stewart*. 2005 WL 6184235, at *5. The FAC alleges that Defendants made
 18 multiple unauthorized copies of thirteen high-value software applications (valued in the millions
 19 of dollars), distributed those copies amongst numerous employees of two separate entities for
 20 commercial, and used counterfeit license keys to access those copies over 39,000 times, all in
 21 furtherance of a nearly three-year long criminal conspiracy, depriving Synopsys of millions of
 22 dollars-worth of licensing fees. The FAC does not allege a “run-of-the-mill” business dispute, it
 23 alleges a pervasive criminal enterprise of the type RICO is designed to prohibit.¹²

24
 25
 26 ¹¹ See also *United States v. Bily*, 406 F. Supp. 726, 730, 733 (E.D. Pa. 1975) (discussing
 “character of the alleged crime” as “infringement for profit”); *but see Stewart v. West*, 2013 U.S.
 Dist. LEXIS 194238, at *15 (C.D. Cal. Sept. 6, 2013) (following *Stewart*).

27 ¹² Notably, in *Stewart*, the court discussed cases involving violations of the federal counterfeit
 28 labeling statute, 18 U.S.C. § 2318 (Section II, *supra*), as examples of cases that would fit within
 the *Stewart* framework.

1 **C. The FAC Alleges Use of Interstate Wires in Furtherance of the Enterprise**

2 To allege a violation of the wire fraud statute, it is necessary to show (1) the formation of
3 a scheme or artifice to defraud, (2) use of interstate or foreign wires in furtherance of the scheme,
4 and (3) specific intent to deceive or defraud. *United States v. Pelisamen*, 641 F.3d 399, 409 (9th
5 Cir. 2011). The requirement of specific intent is satisfied by “the existence of a scheme which
6 was ‘reasonably calculated to deceive persons of ordinary prudence and comprehension,’ and this
7 intention is shown by examining the scheme itself.” *United States v. Green*, 745 F.2d 1205, 1207
8 (9th Cir. 1985), *cert. denied*, 474 U.S. 925 (1985) (internal citations omitted).

9 Defendants misapprehend the scope of wire fraud under section 18 U.S.C. § 1343. The
10 federal wire fraud statute does not require a specific fraudulent statement to be transmitted over
11 the interstate wires, rather, it requires only that the interstate wires be used in furtherance of a
12 fraudulent scheme. As discussed below, the FAC adequately alleges a fraudulent scheme under
13 Rule 9. Thus, the only question presented is whether Defendants used the wires in furtherance of
14 that scheme. Synopsys alleges that Tsai, Ubiquiti, and UNIL used the wires with the intent to
15 engage in their fraudulent scheme of pirating Synopsys’ software, in violation of 18 U.S.C.
16 § 1343. “One ‘causes’ use of . . . wire communications where such use can reasonably be
17 foreseen, even though not specifically intended.” *United States v. Cusino*, 694 F.2d 185, 188 (9th
18 Cir. 1982). A wire communication is “in furtherance” of a fraudulent scheme if it is “incident to
19 the execution of the scheme,” *United States v. Lo*, 231 F.3d 471, 478 (9th Cir. 2000), meaning
20 that it “need not be an essential element of the scheme, just a ‘step in the plot.’” *United States v.*
21 *Garlick*, 240 F.3d 789, 795 (9th Cir. 2001) (quoting *Schmuck v. United States*, 489 U.S. 705, 711
22 (1989); *accord United States v. Garner*, 663 F.2d 834, 838 (9th Cir. 1981) (explaining that the
23 wire transfer “need only be made for the purpose of executing the scheme”).

24 The FAC describes the multitude of instances where the Defendants used the wires in
25 furtherance of their scheme to deceive and defraud Synopsys for financial gain. For example, on
26 multiple occasions, UNIL (from Taiwan) communicated with Synopsys in furtherance of their
27 scheme to fraudulently induce Synopsys in granting limited access to its software. FAC at ¶¶ 49-
28 51. UNIL also used the Internet to contact Synopsys’ customer support in California to gain tools

1 to work-around access to Synopsys' systems. FAC ¶¶ 55-56. Each of UNIL's representations
 2 advanced its purpose.¹³

3 The FAC also establishes that it was reasonably foreseeable to Defendants that interstate
 4 wires would be used in carrying out their fraudulent scheme. On multiple occasions spanning
 5 from September 2013 through May 2014, Tsai contacted Synopsys via email about Ubiquiti and
 6 UNIL's purported desire to evaluate and license Synopsys' license. FAC ¶¶ 35-42, 46, 55.
 7 During this same period, Tsai traveled to Taiwan and continued to represent to Synopsys that
 8 Ubiquiti and UNIL were interested in licensing the software. FAC ¶¶ 40, 50. Included in these
 9 fraudulent email communications were other UNIL semiconductor design employees located in
 10 Taiwan. FAC ¶ 49. At all times relevant to their scheme, Defendants contemplated that any
 11 software that Tsai or Ubiquiti acquired would be transported via wires to UNIL in Taiwan, and
 12 that is precisely what occurred. And, UNIL itself used the Internet to access Synopsys' servers
 13 located in California to download Synopsys' software. FAC ¶¶ 48, 53-54. Once they obtained
 14 Synopsys' software, the Defendants used the Internet to facilitate their exploitation of it—one of
 15 the ultimate goals of the fraudulent scheme. FAC ¶¶ 55-62.

16 Defendants' focus on two emails that were purportedly only sent intrastate (Dkt. 34 at
 17 16:6-16) is a red herring. As described above, the FAC clearly alleges that Tsai, Ubiquiti, and
 18 UNIL intended to use interstate wires to facilitate their fraudulent scheme at least by using the
 19 wires to communicate in furtherance of their scheme and by transferring the critical objects of the
 20 scheme—software copies and licenses keys—internationally over the Internet. *United States v.*
 21 *Lothian*, 976 F.2d 1257, 1262 (9th Cir. 1992) (stating that use of wires exists where one acts with
 22 knowledge that the use of wires will follow in the ordinary course of business or where such use
 23 can reasonably be foreseen); *United States v. Shipsey*, 363 F.3d 962, 971 (9th Cir. 2004) (stating
 24 that the totality of the government's evidence established that the interstate wirings were caused
 25 to occur based on the defendant's fraudulent misrepresentations).

26
 27 ¹³ Although Synopsys has alleged that each of these representations was fraudulent, the use of the
 28 wires may be in furtherance of a scheme to defraud, even where the transmission itself is not
 fraudulent or false, where the use serves some purpose that advances the fraud or contributes to
 the success of the scheme. *Schmuck v. United States*, 489 U.S. 705, 710-11 (1989).

D. The FAC Alleges a Pattern of Racketeering Activity

A pattern of racketeering activity requires at least two related predicate acts that “amount to or pose a threat of continued criminal activity.” *Kearney v. Foley & Lardner, LLP*, 607 F. App’x 757, 758 (9th Cir. 2015) (unpublished, quoting *H.J. Inc. v. Nw. Bell Tel. Co.*, 492 U.S. 229, 239 (1989)). A valid claim must allege predicate acts that “amount to or pose a threat” of continued activity by alleging either (1) “a series of related predicates extending over a substantial period of time;” or (2) “past conduct that by its nature projects into the future with a threat of repetition.” *Religious Tech. Ctr. v. Wollersheim*, 971 F.2d 364, 366 (9th Cir. 1992). Here, the FAC alleges both types of illegal conduct.

First, the FAC alleges a continuing criminal piracy scheme spanning from October 2013 to June 2016, a period of almost three years during which Defendants made numerous fraudulent representations to gain continued access to Synopsys’ software and then trafficked and used counterfeit license keys to illegally access over a dozen copyright-protected Synopsys software applications *more than 39,000 times*.¹⁴ These allegations are clearly sufficient to support a continuous pattern of illegal activity. “More than two years amounts to a substantial period of time to satisfy the closed-ended continuity requirement.” *Kearney*, 607 F. App’x at 759 (citing *Allwaste, Inc. v. Hecht*, 65 F.3d 1523, 1528 (9th Cir. 1995)).

Second, the FAC alleges predicate acts that by their nature project into the future with a threat of repetition.¹⁵ Defendants still possess unauthorized copies of Synopsys’ software, still have the tools and know-how required to create and use counterfeit license keys, and still employ the same individuals responsible for the criminal conduct at issue, including supervisory personnel like Defendant Tsai. *United States v. Philip Morris USA Inc.*, 566 F.3d 1095, 1109

¹⁴ Defendants’ argument that “the complaint does not even state a date range” for Defendants’ predicate acts is simply untrue. In addition to alleging the multiple predicate acts from October 2013 to March 2014 discussed in Defendants’ brief, the FAC also alleges that (1) Defendants began making and distributing unauthorized copies of Synopsys software from approximately December 2013 to April 2014 (FAC ¶¶ 42, 48, 56); (2) began using counterfeit keys in February 2014; (3) began trafficking counterfeit and illicit license keys in March and April 2014; and (4) continuously trafficked and used counterfeit keys to access Synopsys software from March 2014 until June 2016. (FAC ¶¶ 28, 29).

¹⁵ Defendants’ wrongful conduct may be ongoing; discovery is needed to confirm all access to Synopsys’ software by Ubiquiti, UNIL, Tsai and other employees has truly ceased.

(D.C. Cir. 2009) (finding risk of future RICO violations where defendants “businesses presented continuing opportunities to commit RICO violations, and their corporate leadership” remained the same); *Tabas v. Tabas*, 47 F.3d 1280, 1296 (3d Cir. 1995) (risk of future RICO violations where FAC alleged conduct suggesting predicate acts were “an ongoing way of doing business” for defendants); *Nsi Tech. Servs. Corp. v. NASA*, 1996 U.S. Dist. LEXIS 22455, at *10 (N.D. Cal. May 13, 1996) (finding future risk where company misappropriated proprietary information in order to bid on public contract). The fact that Defendants may have temporarily halted their piracy activities because they were caught by Synopsys does not foreclose future misconduct. *Id.* (“the only reason that Serv-Air’s racketeering ended was that NSI informed law enforcement officials of Serv-Air’s criminal conspiracy. Otherwise, Serv-Air might have continued to misappropriate NSI’s proprietary data . . . Fortuitous interruption of a criminal scheme such as this does not preclude a finding of open-ended continuity”) (citing *Allwaste*, 65 F.3d at 1529).¹⁶

E. The FAC Alleges Distinct RICO Enterprises

The FAC alleges multiple distinct RICO Enterprises that support two alternative RICO theories. First, the FAC alleges that Ubiquiti and UNIL are legitimate businesses that carry out normal business activities and that are separate from the criminal activity underlying Synopsys’ claims. FAC ¶¶ 2-9. The FAC further alleges that Tsai and other employees of Ubiquiti and UNIL agreed to conduct the affairs of Ubiquiti and UNIL through a course of racketeering activity that involved criminal copyright infringement and use and trafficking of counterfeit access devices and counterfeit and illicit labels. FAC ¶ 29. These allegations establish the existence of persons (Tsai and other employees) who are separate from the RICO enterprises (Ubiquiti and UNIL). *E.g.*, *United States v. Kirk*, 844 F.2d 660, 664 (9th Cir. 1988) (“existence of a corporation fulfills the requirements of an ascertainable structure apart from the predicate racketeering activity. . . Here, the government presented evidence of several lawful entities existing separately from the racketeering activities”); *United States v. Feldman*, 853 F.2d 648, 660 (9th Cir. 1988) (“The corporate entities had a legal existence separate from their participation

¹⁶ “Because [Synopsys] alleged that the predicate acts amounted to a substantial period of time, [Synopsys] was not required to allege that the acts posed a threat of continued criminal activity.” *Kearney*, 607 F. App’x at 759 (citing *H.J. Inc.*, 492 U.S. at 241-42).

1 in the racketeering, and the very existence of a corporation meets the requirement for a separate
 2 structure. Each functioned to achieve objectives that were not illegal”); *United States v. Blinder*,
 3 10 F.3d 1468, 1474 (9th Cir. 1993) (citing *Bennett v. Berg*, 685 F.2d 1053, 1060-61 (8th Cir.
 4 1982) for the proposition that “Legal entities are garden-variety ‘enterprises’ which generally
 5 pose no problem of separateness from the predicate acts.”).

6 Separately, the FAC also alleges an association-in-fact enterprise (the Piracy Enterprise)
 7 comprising Ubiquiti, UNIL, Tsai, and others. FAC ¶ 123. With respect to the Piracy Enterprise,
 8 Tsai, Ubiquiti, UNIL, and others are the “persons” distinct from the RICO enterprise. Because
 9 the FAC alleges that Ubiquiti and UNIL engage in legal activities separate and apart from the
 10 racketeering pattern underlying Synopsys claims, these allegations are independently sufficient to
 11 establish distinctiveness of the enterprise. *Blinder*, 10 F.3d at 1474 (finding that where the
 12 conduct of at least one of the defendant entities comprising an association in fact enterprise was
 13 engaged in legal activities, the most stringent “separate existence” standard was met) (citing
 14 *United Energy Owners Comm., Inc. v. United States Energy Mgmt. Sys., Inc.*, 837 F.2d 356, 363
 15 (9th Cir. 1988)).

16 Defendants’ sole case, *Ice Cream Distribs. of Evansville, LLC v. Dreyer’s Grand Ice*
 17 *Cream, Inc.*, 2010 U.S. Dist. LEXIS 99930, at *12 (N.D. Cal. Sept. 10, 2010), is inapposite. In
 18 that case, the plaintiff pled that the same three corporations were both the RICO “persons” and the
 19 RICO enterprise, despite the district court’s prior ruling giving plaintiff leave to amend this
 20 pleading deficiency. Defendants’ argument is confusing, but to the extent Defendants argue that
 21 they cannot form an “enterprise” because they are part of the same corporate family, that
 22 argument is foreclosed by Ninth Circuit law. *See Webster v. Omnitrition Int’l, Inc.*, 79 F.3d 776,
 23 787 (9th Cir. 1996) (corporate affiliates can form RICO conspiracies); *Monterey Bay Military*
 24 *Hous., LLC v. Pinnacle Monterey LLC*, 116 F. Supp. 3d 1010, 1046 (N.D. Cal. 2015)
 25 (distinguishing *Ice Cream* and rejecting Defendants’ exact same argument, holding that
 26 “Defendants cannot shed their other corporate distinctions when it suits them, particularly where
 27 it is alleged that the separate corporate entities were critical in carrying out the racketeering
 28 activity”).

1 **IV. SYNOPSYS ALLEGES A RICO CONSPIRACY**

2 Section 1962(d) prohibits conspiracy to violate the RICO statute. The FAC alleges that in
3 or about October 2013, Tsai, Ubiquiti, and UNIL conspired to form a Piracy Enterprise and to
4 operate the enterprise through a pattern of racketeering. FAC ¶ 127. The FAC further alleges that
5 Tsai, Ubiquiti, and UNIL took steps in furtherance of this conspiracy, including by making and
6 distributing unauthorized copies of Synopsys' software and documentation, and using counterfeit
7 and illicit license keys and counterfeit access devices to access Synopsys copyright protected
8 software, among other wrongful acts. *Id.* Contrary to Defendants' argument, the FAC does not
9 allege a "conspiracy of one." Discovery will reveal the names of the other persons involved in the
10 conspiracy.

11 **V. SYNOPSYS ADEQUATELY ALLEGES FRAUD AND NEGLIGENT**
12 **MISREPRESENTATION**

13 In California, the elements for fraud are (a) misrepresentation; (b) knowledge of falsity;
14 (c) intent to defraud, *i.e.*, to induce reliance; (d) justifiable reliance; and (e) resulting damage.
15 *Lazar v. Superior Court*, 12 Cal. 4th 631, 638 (1996). Fraudulent intent is an issue for the trier of
16 fact to decide. *Locke v. Warner Bros., Inc.*, 57 Cal. App. 4th 354, 368 (1997). Negligent
17 misrepresentation, on the other hand, requires a showing of (a) a misrepresentation, (b) without
18 reasonable grounds for believing it to be true, (c) with the intent to induce another's reliance, (d)
19 where there is justifiable reliance, and (e) resulting damage. *Apollo Capital Fund, LLC v. Roth*
20 *Capital Partners, LLC*, 158 Cal. App. 4th 226, 243 (2007). Negligent misrepresentation is
21 narrower than fraud, as it lacks the element of intent to deceive. *Platt Elec. Supply, Inc. v. EOFF*
22 *Elec., Inc.*, 522 F.3d 1049 (9th Cir. 2008) (interpreting California law and stating that negligent
23 misrepresentation is found even where a party makes a representation believing it to be true, if the
24 representation is false and the representation was made without reasonable grounds for the belief).
25 The FAC satisfies both.

26 **Particularity.** A party meets the Rule 9(b) pleading standard if it sufficiently alleges "the
27 circumstances constituting fraud so that the defendant can prepare an adequate answer from the
28 allegations." *Semegen v. Weidner*, 780 F.2d 727, 734-35 (9th Cir. 1985) (plaintiff sufficiently

pleaded fraud claims by alleging “time, place and nature of the alleged fraudulent activities”). Synopsys’ allegations enable Defendants to prepare an answer by providing the time, place and nature of the fraudulent activity. Nothing more is required.

The FAC describes the circumstances of Defendants’ fraud in great detail. For example, the FAC alleges the following false statements:

- On September 30, 2013, Tsai emailed Synopsys in Mountain View and represented that Ubiquiti was interested in taking a total of 21 licenses for Synopsys VCS, Verdi, Design Compiler, and Formality EDA applications during the period from November 2013 to June 2014. FAC ¶ 36.
- On October 1, 2013, Tsai emailed Synopsys in Mountain View and represented that Ubiquiti’s evaluation licenses would be used by a small U.S. team. Tsai stated “I don’t think it’s necessary for us to have the flexibility of checking out licenses across [different physical] sites over [a Wide Area Network].” FAC ¶ 37.
- On October 14, 2013, Tsai emailed Synopsys in Mountain View and represented that Tsai intended for Ubiquiti to consummate its first EDA tool purchase from Synopsys before October 31, 2013. FAC ¶ 38.
- On October 14, 2013, Tsai expressly represented that he would be “the one doing the eval” on his own personal laptop. FAC ¶ 39.
- On December 2, 2013, Tsai emailed Synopsys in Mountain View and stated that he was having trouble running Synopsys’ license management software and temporary key file, purportedly on a virtual machine running on a computer located at Ubiquiti’s San Jose headquarters. Tsai deceived Synopsys into switching the Host ID listed in Ubiquiti’s temporary key file by stating that the prior Host ID information he had provided was for an old personal laptop. FAC ¶ 46.
- At least Tsai and other UNIL employees attended a meeting with Synopsys on or about April 8, 2014, during which Tsai and others represented to Synopsys that access to temporary evaluation license keys for Synopsys’ software could sway UNIL to license Synopsys’ EDA tools. . FAC ¶ 50.
- On May 19, 2014, a UNIL employee contacted Synopsys’ customer support via email for assistance in using tools that, unbeknownst to Synopsys, were secretly being copied and used without authorization by the Piracy Enterprise. The person who made this request on behalf of UNIL represented to Synopsys that time was of the essence, and that finding a quick solution to the subject issue could cause UNIL to license Synopsys’ tool. FAC ¶ 55.

In light of these detailed allegations identifying the parties, the dates, and the general content of the communications, Defendants have adequate notice of the predicate communications and their contents. *See, e.g., Blake v. Dierdorff*, 856 F.2d 1365, 1369 (9th Cir. 1988) (Rule 9(b) met where FAC alleged mail and wire fraud in furtherance of a common scheme and identified specific acts and perpetrators of each); *Ferleger v. First Am. Mortg. Co.*, 662 F. Supp. 584, 588

(N.D. Ill. 1987) (“Rule 9(b) does not necessarily require a plaintiff to specifically describe each mailing in the [FAC]” where time, place, and nature is alleged) (citing *Haroco, Inc. v Am. Nat. Bank and Trust Co. of Chicago*, 747 F.2d 384, 405 (7th Cir. 1984)); *Flood v. Makowski*, 2004 WL 1908221, at *14 (M.D. Pa. Aug. 24, 2004) (“Although Plaintiffs’ [FAC] does not expressly identify how each particular mail or wire communication furthered the scheme, the [FAC] clearly alleges facts which create an unquestionable inference that the alleged communications furthered the scheme”).

Materiality. Despite knowing the exact communications at issue, Defendants argue that Synopsys does not allege with particularity how the statements were material and that some of the statements are not actionable because they are false by “omission.” Both arguments fail. A false statement is “material if it has a natural tendency to influence, or [is] capable of influencing, the decision of the decision-making body to which it was addressed.” *Neder v. United States*, 527 U.S. 1, 16 (1999). Moreover, Synopsys has adequately plead that each of Tsai, Ubiquiti, and UNIL’s statements were material because each empty promise influenced Synopsys to enter into non-disclosure and evaluation licensing arrangements Synopsys would not have otherwise entered. FAC ¶¶ 40, 43. Defendants’ knowingly fraudulent statements further influenced Synopsys into providing Tsai with temporary login credentials, which granted Tsai access to Synopsys’ systems. FAC ¶¶ 44, 113. Synopsys would not have entered into these agreements or offered access to Synopsys’ systems had Synopsys known that the Defendants’ representations were false. FAC ¶ 55.

Misrepresentation by Omission. Defendants’ next attempt to muddy the waters by conflating a misrepresented intention with an omission of a material fact. Case law is clear that fraud exists where one party makes an affirmative representation without the intention to perform on that representation. *See Cisco Systems, Inc. v. STMicroelectronics, Inc.*, 77 F. Supp. 3d 887, 897 (N.D. Cal. 2014) (stating that if a promise to perform is made without the intention to perform, there is “an implied misrepresentation of fact that may be actionable fraud”); *Synapsis, LLC v. Evergreen Data Systems, Inc.*, 2006 WL 44239, at *7 (N.D. Cal. Jan. 9, 2006) (“[A] claim for promissory fraud does not require that the defendant have a specific duty to disclose. Instead,

1 it requires that the defendant have made a promise which the defendant did not intend to keep at
 2 the time it was made, which induced the plaintiff to enter into a contract.”). Fraud may also be
 3 found by volunteering a “half-truth” calculated to deceive. *See Barnes & Noble, Inc. v. LSI*
 4 *Corp.*, 849 F .Supp. 2d 925, 936 (N.D. Cal. 2012) (stating that where a party volunteers
 5 information, the telling of a half-truth calculated to deceive is fraud).

6 Synopsis alleges that each of Tsai’s statements were untrue and calculated to deceive
 7 Synopsis. Tsai knowingly deceived Synopsis by representing that Ubiquiti and UNIL were
 8 ready and willing to enter into a licensing agreement for Synopsis’ software. Tsai’s statements
 9 represented an intention to perform – i.e., to enter into a license agreement and comply with the
 10 license terms. However, Tsai’s repeated affirmative misrepresentations were knowingly
 11 fraudulent and made without such an intention, since Tsai knew that Ubiquiti and UNIL never
 12 intended to license Synopsis’ software but had conspired instead to pirate the software. *Oracle*
 13 *Am., Inc. v. Service Key, LLC*, 2012 WL 6019580, at *8 (N.D. Cal. Dec. 3, 2012) (FAC
 14 adequately pled fraud where Defendant accessed Oracle’s software with the intent to use it for
 15 unauthorized uses); *Compliance Servs. of Am., LLC v. Houser Holdings, LLC*, 2013 WL 4169119,
 16 at *7 (N.D. Cal. Aug. 9, 2013) (claim for fraud existed where Defendants entered agreement
 17 without any intention of performance); *Sussex Fin. Enters., Inc. v. Bayerische Hypo-und*
 18 *Vereinsbank*, 2010 WL 94272, at *5 (N.D. Cal. Jan. 6, 2010) (allegations of wire fraud were
 19 sufficient where Defendants affirmed an intention to issue loans that could last thirty years, but
 20 allegedly never intended to do so); Cal. Civ. Code § 1710, subd. (4) (defining false promise by
 21 statute as “[a] promise, made without any intention of performing it”). As stated by the court in
 22 *Glendale Fed. Sav. & Loan Ass’n v. Marina View Heights Dev. Co.*, “[A] promise to do
 23 something necessarily implies the intention to perform, and, where such an intention is absent, it
 24 is an implied misrepresentation of fact, which is actionable fraud.” 66 Cal. App. 3d 101, 133
 25 (1977).

26 **Damages.** Defendants’ argument that Synopsis did not plead damages with particularity
 27 is another red herring. Rule 9(b) does not require that fraud damages be pled with particularity.
 28 *See, e.g., Andrews Farms v. Calcot, Ltd.*, 527 F. Supp. 2d 1239, 1252 (E.D. Cal. 2007) (“While

1 Rule 9(b) requires pleading the circumstances of fraud with particularity, defendants cite no case
 2 law, and the Court finds none, requiring that fraud damages be pled with more specificity than
 3 required under normal notice pleading.”); *Menjivar v. Trophy Props. IV DE, LLC*, 2006 WL
 4 2884396, at *13 (N.D. Cal. Oct. 10, 2006) (same); *Chaghouri v. Wells Fargo Bank, N.A.*, 2015
 5 WL 65291, at *4 (N.D. Cal. Jan. 5, 2015) (none of the Ninth Circuit’s formulations of the FRCP
 6 9(b) requirements require damages to be pleaded with particularity); *Ward v. Nat’l Entm’t*
 7 *Collectibles Ass’n*, 2012 WL 12885073, at *6 (C.D. Cal. Oct. 29, 2012) (collecting cases).
 8 Nevertheless, Synopsys does in fact plead that it was damaged as a result of Defendants’ conduct
 9 in the form of misappropriation of valuable intellectual property, lost licensing revenue, and costs
 10 associated with remediating [Defendants’] conduct. FAC ¶¶ 29, 133.

11 CONCLUSION

12 For the foregoing reasons, Defendants’ motion to dismiss should be denied.

13
 14 Dated: April 25, 2017

DENISE M. MINGRONE
 ROBERT L. URIARTE
 ORRICK, HERRINGTON & SUTCLIFFE LLP

15
 16
 17 By: /s/ Denise M. Mingrone
 18 DENISE M. MINGRONE

19 Attorneys for Plaintiff/Counterdefendant
 20 SYNOPSIS, INC.